Performance Work Statement (PWS)

FOR

Activity Manpower Management (AMM)

(Total Force Manpower Management System (TFMMS) Modernization)

Sea Warrior Program Office

PMW 240

Sea Warrior
PROGRAM
PMW 240

eSolutions for Sailor and Fleet Readiness

TABLE OF CONTENTS

1 Introduction

The Department of the Navy (DON) initiated an effort to improve organizational effectiveness by integrating Activity Manpower Management (AMM) processes across directorates and commands. This effort is to provide a seamless and more centralized approach to manage AMM activities that will: reduce duplication of effort and process times; reduce costs; ensure easier compliance with policies, regulations and standards; and improve decision making. These objectives will be accomplished by an AMM system that is agile and flexible in response to changing business needs, and improves enterprise accessibility as well as the accuracy and consistency of manpower data. The results of this effort will strengthen and right-size the Department of Defense (DoD) Total Workforce mix (military, civilian, and contracted support) to accomplish the DoD mission and sustain superior performance.

The DON leadership requires an agile and intuitive system to meet Navy AMM goals and objectives by reducing errors in manpower transaction processing by 50% and streamlining business processes by reducing duplicative tasks and optimizing workflow. This effort will define and structure manpower business requirements to comply with DoD/Chief of Naval Operations (CNO) Information Management initiatives. The Business Process Reengineering effort will allow stakeholders to have direct input to business requirements that increase visibility, availability, and usability of AMM information. Additionally, this effort will provide an integrated AMM workflow capability to increase process efficiency and stakeholder confidence in AMM products and services.

The Sea Warrior Program (PMW 240) is the primary Information Technology (IT) acquisition agent for non-tactical business operations addressing manpower, personnel, training and education (MPTE) capability gaps, legacy systems, and Distance Support to the Fleet. The PMW 240 Program manages a complex portfolio of systems that enable the Navy to perform Human Resources (HR) and other non-tactical business operations ashore and afloat. The PMW 240 Program is part of the Navy Program Executive Office for Enterprise Information Systems (PEO-EIS), which develops, acquires, and deploys seamless enterprise-wide IT systems with full lifecycle support for the warfighter and business enterprise.

PMW 240 is acquiring development services to modernize the Total Force Manpower Management System (TFMMS) for the AMM effort.

1.1 Current Systems

The current TFMMS capability includes a legacy mainframe TFMMS and a TFMMS Micro Manpower Change Application (TMMCA) (a subset of TFMMS capabilities in a classified and unclassified environment). The TMMCA is a web application that consists of an Internet Information Services (IIS) Web Server front end, a JavaBeans Open Source Software (JBOSS) middle tier and an Oracle database. The web application software is written utilizing Java and HTML.

TFMMS includes current capabilities of Manpower Change Request (MCR), Billet Change Request (BCR) management, End Strength Processing/Management, Activity Management, Officer/Enlisted Programmed Authorization (OPA/EPA) management, Budget Exhibit Submissions, Inherently Governmental and Commercial Activity Inventory Management, Joint Manpower Crosswalk mapping, Navy Manpower Planning Programming Budgeting and Execution (PPBE) submission and processing, Activity Distribution Process (AD) and Activity Priority Manning Process (AP), Manpower Data Products (interfaces, reports, etc.), and maintain data validity (validation tables, business rules).

TFMMS currently supports a user base of 2,200 Manpower Professionals who maintain manpower data for 9,718 activities and annually complete 1.2 million transactions in the system.

The legacy TFMMS architecture, including the database structure, requires a significant effort to develop, test and deploy updates driven by business process changes. AMM processes are currently supported by a mixture of information technologies. Some Programmed Authorization business processes are conducted in systems outside of TFMMS in order to support the business requirements. Manpower transactions are managed by TFMMS, while other functions are managed by custom algorithms and Microsoft Access© databases, including Programmed Manpower Authorization System (PMAS), Spreadsheets.mbd, and TFMMS, Table, Future Years Defense Program (FYDP) & Activity Maintenance Software (TTFAMS). The use of these databases require that the current TFMMS data be downloaded, formatted, and uploaded each time they are updated and used for production of manpower related products.

A modernized architecture is needed to eliminate manual work-arounds, support auditing of transactions to the billet level or Letter of Justification (LOJ), and to simplify and consolidate manpower transactions and data.

2 Scope

This Performance Work Statement (PWS) defines the scope of this PEO-EIS PMW 240 task for the design, development, integration, test, implementation and sustainment of the TFMMS Modernization that includes existing capabilities and the requirements identified in the AMM Functional Requirements Document (FRD).

Navy Total Force Manpower requires a web-based, real-time environment be established for TFMMS. The technically refreshed system needs to provide a high-level ability to conduct mass data updates based on policy changes, data element changes, business process changes, etc. to increase its agility. The system must provide an ad hoc reporting capability. Activity Manpower Management needs the ability to provide leadership accurate and real-time reporting on Manpower and Force Structure to allow for informed business decisions.

TFMMS requires a modern data warehousing capability which standardizes audit tracking, ad hoc reporting, and provides an efficient and accessible history / archive capability. An automated method for the transfer of data from completed Navy Manpower Requirements System (NMRS) manpower documents into Manpower Changes in TFMMS is required.

The system must be developed such that the system functions are intuitive and utilize standard, consistent business rules.

Based on the approved strategy, modernization will be performed using the recently technically upgraded TMMCA application in two phases:

1. Billet Change Request (BCR), Activity Maintenance
2. Manage End Strength, Authorize Position, Extended Workflow, Manage Level of Aggregation (LOA), Reports, and Interfaces

This solution will use the technically refreshed TMMCA web application as the foundation for the TFMMS Modernization. Utilizing TMMCA as a foundation for TFMMS Modernization will maximize reuse of existing functionality and data that currently resides in both systems. Functionality shall be consolidated into one system minimizing interfaces and maximizing data accuracy. Functionality shall be added in order to fulfill all detailed requirements outlined in the AMM FRD.

The current TMMCA web application consists of an IIS Web Server end, a JBOSS middle tier and an Oracle database. The web application software is written utilizing Java and HTML. The modernized TFMMS application, also referred to as TFMMS Modernization, will have a classified and unclassified environment. It will leverage the TMMCA classified and unclassified environments, but will provide an enhanced mechanism to transfer data between both environments utilizing a device such as Radiant Mercury. TMMCA is currently hosted in the New Orleans Data Center.

The Contractor shall deliver a fully functioning TFMMS Modernization system that will continue to be hosted in the New Orleans Data Center.

The Contractor shall satisfy all the requirements of the FRD. The Contractor shall also follow the guidance for technical events and documentation identified in the PMW 240 Program Office Technical Event Process (TEP) as tailored and documented in the TFMMS Web Integrated Master Plan (IMP). General Systems Engineering activities as outlined in section 3 of this PWS are applicable for modernization tasks as well as maintenance updates.

The Contractor shall perform to the requirements of this PWS and adhere to all of the policy and regulations associated with DoD Business Systems, the DoD network connections, and the hosting facility.

The program includes: Initiation, Planning, Development and Acquisition, Testing, and Deployment and Sustainment. Within these activities, all engineering, development, testing, deployment, and sustainment will be conducted in accordance with the Navy PEO-EIS Systems Engineering Technical Requirements (SETR) and Technical Event Process (TEP) guidance. Appropriate technical, functional, and stakeholder reviews and acceptance will be conducted in accordance with the SETR and TEP.

This contract includes general Engineering Services in support of the TFMMS program, including Professional Services and Subject Matter Expertise (SME) support.

2.1 Development and Acquisition Phase

This effort includes requirements analysis, design, development, test, and operational deployment. General requirements for these activities are included in section 3 of this PWS in addition to the following.

The requirements analysis will consist of the development of the System Requirements Specification (SRS) IAW **CDRL A003**, and the System Subsystem Specification (SSS) IAW **CDRL A002** in preparation for the System Requirements Review/System Functional Review (SRR/SFR).

The design phase will consist of application and database design for all detailed requirements identified in the SRS. Design will meet the performance criteria identified in the SSS. Output of the design phase includes menu, screen, and report layouts for each functional component of the application. The design phase also consists of the development of the conceptual database design, identification of the application architecture, identification of required user roles, and any additional design that is needed in preparation for the Preliminary Design Review (PDR). Development of the System Design Document (SDD) IAW **CDRL A004** shall begin during the design phase, and is finalized prior to the Critical Design Review (CDR).

The development phase will consist of the database and application development, unit test, integration test, regression test, performance test, functional test, and deployment of all software components.

2.2 Sustainment

Sustainment includes all activities, products, and services required to keep a system running so that it is operationally available to the functional user for approved service levels. This includes: bug fixes, required hardware and software license maintenance, security, planning, management, configuration management activities, and development and maintenance of documentation. It includes system and database administration functions to maintain a system’s operation and availability.

In addition to day-to-day operations and bug fixes sustainment also includes minor upgrades and modifications in response to Change Requests (CRs) or trouble reports that relate to changes in process, policy, and interface changes, that meet DoD and DON interoperability, information assurance, data protection requirements as well as to maintain currency with software engineering and design best practices as required by DoD and DON.

Sustainment may include products and/or services provided by a teaming partner/subcontractor. A description of general sustainment and maintenance tasks are identified in Section 3 of this PWS.

2.3 Government Furnished Property (GFP)/Government Furnished Equipment (GFE)

Hardware and software for existing systems will be provided by the Government as necessary for modernization efforts. TFMMS Modernization environments for Development, Test, and Production will be hosted in the SPAWAR SYSTEMS CENTER ATLANTIC New Orleans Data Center.

The Government shall provide existing TMMCA source code, user/admin manuals, system documentation, including design documentation and technical data that is available after contract award.

2.4 User Base and Access

The Contractor shall deliver TFMMS Modernization to support Navy and Marine Corps personnel via the ashore Continental United States (CONUS) and Outside Continental United States (OCONUS) infrastructure. The Contractor will develop the TFMMS Modernizatoin system so that it is accessible directly through the World Wide Web.

Users will access the system from classified and unclassified environments on any computer via the Naval Enterprise Networks (NEN), to include Navy Marine Corps Intranet (NMCI) Next Generation Enterprise Network (NGEN), Non-classified Internet Protocol Router Network (NIPRnet), and Secret Internet Protocol Router Network (SIPRnet).

2.5 Data Integrity and Accuracy

Associated with all modernization and sustainment/maintenance activities, the Contractor is responsible for maintaining the integrity, security and accuracy of the data. The Contractor shall ensure the quality of data across the development, test, and production environments, while maintaining configuration control for each of these environments.

3 General Requirements

The Contractor shall perform work necessary to meet the PWS and TFMMS Modernization functional requirements. The Contractor shall deliver products in accordance with (IAW) the Contract Data Requirements Lists (CDRLs) as specified.

When applicable and as approved by the Government, the Contractor shall update existing documentation before developing new documents.

The Contractor shall support delivery and operation of a fully functioning and deployable system that:

- Ensures all updated versions are compatible/interoperable with earlier versions. This includes through the phased development as well as updates after final production.
- Ensures continuity for interfaces and data exchange with designated external systems, and coordination of concurrent changes with interface partners.
- Provides the necessary deployment planning, installation verification, and testing to ensure each technical solution works within the system environment.
- Abides by Government standards, regulations, and policy, including those identified in Appendix C.
- Ensures the software release package and supporting documentation shall be comprehensive enough to facilitate package installation, data migration, operation and sustainment by the existing Government workforce or third-party designee.

3.1 Overarching Functions

The overarching functional areas within this PWS include:

- requirements analysis
- design
- development
- integration
- testing
- sustainment/maintenance

Descriptions of the general activities the Contractor shall accomplish in each of these areas are identified in the following sub-paragraphs. These activities are tailorable according to the magnitude of the effort required, and as approved by the Government. It should be noted that while the terms of design, development, integration, and testing are used and normally are associated with development/modernization, they also apply to activities associated with CRs as part of sustainment activities.

The Contractor is responsible for all aspects of system security as described in section 6 of this document. This includes Information Assurance Vulnerability Management (IAVM) updates and break/fix activities, as well as providing all necessary Certification and Accreditation (C&A) Documentation, **CDRL A00E**.

3.1.1 Requirements Analysis

The Contractor shall perform requirements analysis for all TFMMS Modernization requirements, including those documented in the FRD and the SSS. The Government will provide a draft SSS as GFI. The Contractor shall finalize the SSS IAW **CDRL A002**. Requirements shall be analyzed to ensure the required or requested changes are understood. The Contractor shall provide a SRS IAW **CDRL A003** that includes a decomposition of the SSS, and shall assist in the update of the SSS as necessary. The SRS shall include a list of the Computer Software Configuration Items (CSCIs). The Contractor shall track requirements and provide a Requirements Traceability Matrix (RTM) when required, and IAW the TEP, using the PMW 240 requirements tool and report capability. The Contractor shall use a PMW 240 requirements management tool, if available, for recording and analysis of requirements, and for generating the SSS and SRS reports.

The Contractor shall delivery the Interface Requirements Specifications as part of the SRS, CDRL **A003.**

In addition, the Contractor shall assess requirements associated with CRs or Software Problem Reports (SPRs), and report on the impact the changes will have on the operational performance as well as provide an estimated cost and proposed schedule for the change. The Contractor shall evaluate change requests and where possible recommend combining requirements for more efficient design and development.

The Contractor shall assist in the submission of CR information IAW the Government's Configuration Management Plan and using the Government's configuration management tools.

Additionally, the Contractor shall review the functionality satisfied by the existing systems and previously conducted requirements gap analyses, to ensure the functional requirements across the existing systems is understood to ensure proper migration of functionality to TFMMS Modernization.

3.1.2 Design

The Contractor shall use standard methodologies to develop designs and baseline estimates for maintenance updates to the current system. Design incorporates DoD and Commercial common standards, common architectures, and common parts into a comprehensive product. Design integrates and synchronizes products and services with existing product and service solutions, and considers reuse or reconfiguration of existing software to the maximum extent possible. Design includes integration and synchronization of the resource input from a teaming partner(s) or subcontractor(s) into the final product. Design includes obsolescence screening to assess the supported useful life of proposed software components. Design also includes the incorporation of concepts relative to ease of sustainment and cost savings in the final product and addresses the life cycle requirements of the selected Course of Action (COA).

The Contractor shall deliver all design and associated documentation appropriate for the effort, as well as recommendations for changes. The Contractor shall present the designs and recommendations to the Government for approval in conjunction with technical design reviews. The Contractor designs shall take into account all internal and external interfaces.

The Contractor shall update or develop a SDD IAW **CDRL A004**.

As applicable, Interface Design Descriptions (IDDs) shall be included in the SDD.

3.1.3 Development

Development includes the procurement of materials and personnel, building and assembling of hardware, software and personnel as well as other resources applicable to the product or service design. Development is the standardized processes and procedures by which a contractor transitions a design into a deliverable product. Development integrates products and services provided by a teaming partner or subcontractor, if applicable. Development also includes unit and integration testing of teaming partner or subcontractor provided products and services. Development includes ensuring all necessary components, interfaces, and data migration and exchanges satisfy functional and performance requirements. Development also includes all the associated documentation.

The Contractor shall support testing during development IAW the design, approved by the Government. The Contractor shall develop software components and interfaces using approved software development methodology (e.g. Agile development). Software development can include: adoption, reuse, or reconfiguration of existing software components, implementation of Commercial-Off-The-Shelf (COTS) products, or new software development. The Contractor shall document and provide the overall software development approach in a Software Development Plan (SDP), **CDRL A001**.

3.1.4 Integration

The Contractor shall perform integration of the TFMMS Modernization components. The Contractor shall ensure that all internal and external integration is performed to satisfy all functional and specified performance requirements. External integration includes interfaces and data exchanges with external systems as well as integration with host facilities, platforms, and networks. The Contractor shall ensure that products are compatible and interoperable with all prior versions as necessary. Integration may include products and/or services provided by a teaming partner/subcontractor, or other Government activity. Integration includes the definition, collection, and deployment of test data, data management and migration, deployment plans, installation procedures, system and database administration and operations procedures that enable end-users to acquire the skills and knowledge necessary to effectively use the product and/or service.

3.1.5 Test

The goal of testing is to ensure that the functionality as defined in the project's SRS is delivered as specified in CDRL A003 and that the integrated application(s) perform as expected with minimal defects. Testing throughout the project lifecycle, as described in the PMW 240 TEP, will consist of both Contractor and Government testing events. The test activities that will be performed for the project will be documented in the project's IMP with further elaboration of the test and evaluation strategy within the project's Test and Evaluation Master Plan (TEMP).

The Contractor shall conduct all test planning, preparation, execution, and reporting for Application Unit Testing (AUT). AUT is the functional development testing phase that verifies that the developed application is free from defects and is a candidate for software release. It is recommended, that testing during AUT should represent a complete systems test performed by a Quality Assurance (QA) or Test team. The AUT should adhere to the development organization's standard practices and procedures and will be documented in the SDP. AUT results will be included as part of the presentation at the Application Test Readiness Review (ATRR) as verification of functional development testing.

The SDP, **CDRL A001**, documents the processes, methods and approach for the development and testing of all requirements during the AUT phase. The level of detail in the SDP should be sufficient to define all processes, activities and tasks to be conducted. This includes specific standards, methods, tools, actions, strategies and responsibilities for both the development and testing activities. All test procedures and practices employed during AUT should be fully documented in the SDP. The Contractor will be responsible for successful execution of the developed test scripts in accordance with the criteria defined within the TEMP.

All test events following AUT will be managed by the Government. The Contractor shall coordinate closely with the Government and, if employed, a third party test team, to provide technical support for these test events. This support includes:

- Test event planning
- Test scenario development
- Test environment design
- Test data development
- Test script development (to measure satisfaction of SRS functionality)
- Traceability matrix development (mapping test scripts to SRS requirement(s))

Testing of updates and modifications performed as part of sustainment activities shall include regression testing.

3.1.6 Sustainment

The Contractor shall provide support for all application issues associated with the operation of TFMMS Modernization. The Contractor shall have a team capable of solving issues with the applications and all configuration items.

The Contractor shall provide support for TFMMS Web in the development, test, and production sites to troubleshoot and conduct corrective actions. This also includes the Continuity of Operations (COOP) capability.

Contractor shall maintain/sustain systems IAW system performance requirements of Section 5.7.

The Contractor shall ensure that all sustainment and maintenance updates provide cost-effective capability that fully integrates business processes, tools, and authoritative data.

3.1.6.1 Sustainment Services

The Contractor shall perform the following types of activities as part of day-to-day sustainment and maintenance.

- Sustainment, which includes processes, procedures, people, materiel, and information required to support, maintain, and operate the TFMMS system and associated databases at its core service level. Additionally, sustainment includes documentation, operations, deployment, security (including C&A support), configuration management, training (users and sustainment personnel as required), Tier II help desk, and Commercial-Off-the-Shelf (COTS) product management.
- Maintenance is the process of modifying the TFMMS system application software and database to correct faults (bug fixes, system breakage, and emergency fixes). Maintenance includes:
    - resolving software problem reports and the resolution of outages
    - executing security updates in support of IAVM
    - ensuring products/components operate as required and satisfy performance requirements
    - keeping all production support documentation up to date including: administrator and user documentation, training materials (as required), and other logistics documentation
    - testing and implementation of upgrades/new versions, including Service Packs
    - completing post-production checklists
    - providing technical support to the hosting facility as necessary
- Database Administration, which includes maintaining the logical and physical data models for databases, implementing physical databases, maintaining reference tables and metadata, and providing support to all environments.

- Production Support above the Operating System (OS), which includes services provided by the support staff to perform daily monitoring of program production schedules, interfaces, outputs and operations. This includes responding to situations and issues raised by functional users who require assistance with use of the program or analysis by the support staff to assist the user. Analysis can include such things as system functionality, data anomalies, research for issues and is only in support of system breakage or emergency fix issues that would result in a customer work stoppage.
- Implementation, test, and delivery of system maintenance, and support. Software/System releases resulting from sustainment activities shall be documented and updated in release notes and in appropriate System Documentation.
- Security support, which includes ensuring that the TFMMS Modernization software and database continues to satisfy DoD and Navy regulations and standards, including Information Assurance (IA) regulations, regular Security Technical Implementation Guide (STIG) implementation, and safeguards to ensure continued security compliance and accreditation of the system, environments, and personnel.
- Interface and data exchange support, which includes ensuring continued operations and data exchange across all necessary DoD environments and within communications constraints, including links and interfaces between the TFMMS Modernization and external systems. The Contractor shall ensure that new versions developed function properly with multiple prior versions until those older versions are deprecated.
- Operations support, which includes Tier II help desk support for trouble calls and tracking SPRs until resolved. This includes the collection and reporting of metrics associated with the response and resolution of SPRs. Metrics collection must also include coordination with hosting facility personnel to report on system performance that shall at a minimum include: reliability, availability, maintainability, response times, and utilization. The Contractor shall provide Help Desk support 8 hours a day, five days a week.
- The Contractor shall analyze all SPRs and submit them into the configuration management tool approved by the Government.

3.1.6.2 Minor Sustainment Upgrades

The Contractor shall perform Minor Sustainment Upgrades as part of sustainment and maintenance of TFMMS Modernization. These services include minor software modifications other than break/fix updates that are related to business process and policy changes as well as modularity and open systems architecture improvements. They include modifications to enhance performance or other attributes, or to adapt to advances in technology. Minor System Upgrades include support for submission of CRs in a Government approved tool for configuration management. The Contractor shall also recommend combining requests for changes and fixes to problems as needed into logical blocks for upgrades. It can also include support for the preparation of Levels of Effort and engineering change recommendations to further define the CR and any other documentation needed for approval decisions by the PMW 240 Assistant Program Manager (APM) and a Configuration Control Board (CCB) as required.

These software modifications are typically performed in conjunction with a Class I or II CRs. A Class II CR is generally characterized as minor and can include:

- Cosmetic screen changes
- Business rule or algorithm changes
- Maintenance actions which are isolated only to a single product with no increase in product performance envelope (e.g. addition of new features and services that did not previously exist).
- Can be done within allocated above core budget, schedule and resources
- Modifications to existing data interfaces that do not change the security posture of the product
- Special requests and changes directed by Flag Officers and members of the Senior Executive Service (SES) not meeting Class I criteria

The characteristics of Class I CR preparation that is within scope of Minor System modifications but do not rise to the level of a modernization effort are:

- Changes that have a cascading dependency that impacts interfaces or systems outside a single APM control
- Impacts DoD or Navy policy
- Technology refresh efforts that could result in an incidental change to the performance envelope of the product
- New system interfaces that could change the security posture of the product or that contain privacy sensitive personnel data
- Efforts that breach approved funding baseline for the approved sustainment level of effort
- Product re-factoring needed as a result of an application host facility change or security posture change
- Modularity and open systems architecture improvements that reduce life-cycle costs of the system.

Modifications and updates performed as part of sustainment services shall include testing performed by the Contractor including regression testing, performance testing and installation verification. Testing should represent a complete systems test performed by a Quality Assurance (QA) or Test team.

Regression testing shall be performed by the contractor and ensure that new software releases do not break existing system functionality; automated regression testing scripts shall be delivered to the government IAW **CDRL A00G** and placed under configuration management.

3.2 Place of Performance

The development, testing, integration and deployment work to be performed under this contract shall occur at the SPAWARSYSCEN Atlantic, New Orleans Office, New Orleans, LA.

The Contractor shall provide technical support for the installation and regular exercise of the COOP as directed by the Government. This includes off-site technical support for the COOP implementation.

3.3 Data Deliverables

All CDRL deliverables shall be submitted in a format that is compatible with Microsoft Office 2007 and as specified, in the CDRL. The Contractor shall notify all CDRL addressees, by email, when a CDRL has been delivered on the day CDRL was posted.

The Government shall have Unlimited Data Rights to any software or data products developed under this contract.

3.3.1 Restrictive Markings on Data

The Contractor shall notify the Procuring Contracting Officer (PCO), in writing, prior to or at the time of submission, of any Data to be submitted with anything other than unlimited rights and markings as defined in Federal Acquisition Regulation (FAR) Subpart 27.4 – Rights in Data and Copyrights, and Defense Federal Acquisition Regulation Supplement (DFARS) Subpart 227.71-Rights in Technical Data.

4 Program Management Requirements

The Contractor shall establish and maintain an integrated program management system to plan, direct, integrate, and control the administrative, management, technical, logistical, financial, production, and support functions of each specific task. The Contractor shall manage work efforts to optimize total system performance, promote interoperability and common solutions, and minimize total ownership cost. The Contractor shall measure, monitor, and assess the progress of the work performed and costs incurred under the contract task. The Contractor shall adopt a total system and system of systems approach to product support and structure system by design, testing, support planning, resourcing, and post-fielding.

4.1 Contract Progress, Status, and Management Report Preparation

The Contractor shall submit a monthly Contractor Progress, Status, and Management Report IAW **CDRL B001**. The report shall identify and contain summary-level information on all on-going tasks, to include status of work completed under this PWS and identify any cost, schedule, and performance risks or issues. The report shall include a status of staffing and transition.

As part of sustainment activities, the report shall also include monthly performance metrics including: reliability, availability, maintainability, response times, and utilization.

The Contractor shall provide verbal status of projects/activities as requested by the Government.

4.1.1 MSR Worksheet

Immediately after contract award, the Contractor shall complete the MSR Cost Proposal worksheet that's included in **CDRL B001** as a baseline for cost and schedule. After Government approval of the baseline, the Contractor shall complete and submit the monthly MSR Worksheet that is part of the Contractor's Progress, Status, and Management Report IAW **CDRL B001.** The MSR Worksheet will be used to compare monthly cost and schedule performance to the cost and schedule baseline submitted as part of the Contractor's cost proposal. The Contractor will identify the current monthly and cumulative "to-date" percent of budgeted cost of work scheduled that was performed, actual cost of work performed, and estimate at completion for each Contractor Work Breakdown Structure level reported within their cost proposal.

The MSR Worksheet will enable the Government to monitor monthly cost, schedule and technical performance progress. The monthly inputs shall determine whether cost and schedule variations exceed 10% from the baseline. For cumulative deviations that exceed 10%, the Contractor shall explain the cause of the variance and the corrective actions to be taken if necessary.

The Contractor shall not adjust cost performance data from prior months. Any errors, accounting adjustments or approved re-baseline actions shall be recorded as a single point adjustment in the current reporting month.

4.1.2 Integrated Master Schedule (IMS)

The Contractor shall develop and maintain an IMS IAW the IPMR/IMS **CDRL B007** and the Sea Warrior Program Office Technical Event Process (TEP) Guide. The Contractor shall manage the IMS it has developed by logically networking detailed program activities. The Contractor shall submit IPMR Format 6 on a monthly basis to report critical issues to the Government. The schedule shall contain the planned events and milestones, accomplishments, exit criteria, and activities from contract award to the completion of the contract. The IMS shall include a detailed account of all tasks necessary to accomplish the goals and objectives for each specific task. The IMS shall use the work breakdown structure elements identified in the MRS Worksheet that is part of the Contractor's Progress, Status, and Management Report IAW **CDRL B001** as the foundation for the IMS**.** The Contractor shall quantify risk in hours, days, or weeks of delay and provide optimistic, pessimistic, and most likely duration for each IMS activity and event. The Contractor shall identify dependencies within and external to the Contractor's IMS.

The Contractor shall also provide input into the PMW 240 IMS for the Program. The Contractor shall coordinate with the Government representative for the PMW 240 Program IMS to provide details of all tasks on at least a monthly basis and report critical issues to the Government. The Contractor shall identify potential schedule conflicts and/or problems and recommend solutions.

4.1.3 Enterprise-wide Contractor Manpower Reporting Application (ECMRA)

The Contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for SPAWAR via a secure data collection site. The Contractor is required to completely fill in all required data fields using the following web address: https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://doncmra.nmci.navy.mil."

4.1.4 Function Point (FP) Analysis

PMW 240 uses Unadjusted Function Points (UFPs) to estimate the size of software applications to support project management. UFPs are used for planning (including cost estimation), project execution (monitoring productivity and requirements creep), and sustainment support (monitoring reliability and maintenance costs).

FP Analysis according to the standard practices identified by the International Function Point Users Group (IFPUG) provides a structured technique for identifying functionality from the user's perspective and provides a measure of size for a software application. It categorizes system functions into five classes of transactions and logical files. Internal Logical Files (ILFs) and External Interface Files (ELFs) are where data is stored. External Inputs (EIs), External Outputs (EOs), and External Inquiries (EQs) are transactions against these files. The FP Analysis process identifies these logical files and transactions and calculates a number of FPs for a software system. The resulting number is a size measure that can be used to support cost estimation and monitor other project metrics.

When tasked by the Government, the Contractor shall perform FP Analysis to determine the estimated number of UFPs. The Contractor shall focus on the RMI functional requirements as they are satisfied and measure progress in terms of UFPs in addition to metrics associated with standard requirements management. The Contractor shall report progress in the monthly Contractor Progress, Status, and Management Report IAW CDRL B001. The Contractor shall distinguish the number of the UFPs associated with software customization vs. configuration or direct COTS implementation. At contract completion, the Contractor shall identify the final UFP count for the RMI capabilities as delivered. The contractor shall deliver an UFP report in accordance with **CDRL B009** using contractor format.

4.2 Contractor Performance Assessment Reporting System (CPARS) Draft Approval Document (CDAD)

The Contractor shall submit a CDAD report IAW **CDRL B002**.

4.3 Management Plan

The Contractor shall provide a plan describing the program management system IAW **CDRL B003**. The Management Plan shall consist of the organizational structure, the assignment of functions, duties, and responsibilities, the procedures and policies and the reporting requirements that are established for the initiation, monitoring, control, completion, test, and verification, and reporting of contractual tasks, projects, and programs. The Contractor's organizational structure, methods, personnel, and internal support functions shall be developed describing roles, responsibilities, names and types of personnel assigned, and security required to successfully perform this task. The Management Plan shall also include staffing and transition plan. The Contractor shall also include in the Management Plan, the Contractor's plans for Quality Assurance Program, Risk Management, and Subcontractor Management Report described in the following paragraphs.

4.3.1 Quality Assurance Program Plan (QAP)

The Contractor shall develop a Quality Management Program and describe their processes and procedures for managing the quality of systems and products produced, and specific quality measures that that Contractor will report to the Government on a monthly basis. This information shall be included in the Management Plan, **CDRL B003**. Monthly quality reports are included within the Contractor Progress, Status, and Management Report. The Contractor shall implement a Quality Control Program that meets the requirements for this contract.

4.3.2 Contractor's Risk Management Plan (RMP)

The Contractor shall include a RMP as part of the Management Plan, **CDRL B003**, describing their processes and procedures for implementing an integrated risk management system with risk planning, identification, assessment, mitigation, and monitoring functions to improve technical, cost and schedule performance. Risk shall be identified and described in accordance with the PMW 240 RMP. The Contractor shall description the risks for all activities identified in the work breakdown structure within the cost/schedule report submitted as part of the contract proposal. Progress reporting of risks shall be addressed in the monthly Contractor Progress, Status, and Management Report, **CDRL B001**. The Contractor may opt to use the Government instance of Risk Exchange in support of the RMP.

4.3.3 Subcontractor Management Report

When applicable, the Contractor shall deliver a Subcontractor Report as part of the Management Plan **CDRL B003**, describing their processes and procedures for selecting and managing Subcontractors. This report shall identify the name of the business Subcontractor, the tasks performed, and the associated costs for each, and scheduled availability which will be used to ensure requirements are being met by the Contractor. The Contractor shall integrate Subcontractors into program Integrated Product Teams (IPTs) and Contractors program management processes as applicable.

4.4 Contract Configuration Management (CM)

The Contractor shall deliver a Contractor's Configuration Management Implementation Plan (CMIP), IAW **CDRL A008,** that is consistent with the PMW 240 CM processes and tools. Configuration information including: requirements documents, RTMs, Entity-Relationship Diagrams (ERDs), data dictionary, business rules, data mapping, and draft and final versions of Systems Engineering Documents.

4.4.1 Configuration Management Records/Reports

The Contractor shall implement a Configuration Management Records/Reports effort for Configuration Status Accounting (CSA). The Contractor shall provide and maintain Configuration Management Records/Reports IAW **CDRL A009** and the PMW 240 Configuration Management Plan and using the PMW 240 Configuration Management tools

4.4.2 Baseline Management

The Contractor shall implement baseline management. The Contractor shall propose changes to the product baseline for each configuration item and manage the baselines IAW the CMIP, using the Government approved configuration management process and tools.

The Contractor shall prepare and manage required Functional/Allocated/Product (F/A/P) configuration baselines to include a complete listing of technical documentation, logical configuration items such as CSCI and any change request defining the authorized configuration. The Contractor shall generate a baseline report that lists the current configuration identified for the F/A/P baseline. The baseline CSCI List shall be submitted IAW **CDRL A00B.**

The CSCI List is expected to be used in the planning and design of the software project. CSCI products that are delivered will be specified in the Software Version Description (SVD) IAW **CDRL A00D**.

4.5 Reports, Plans, and Meeting Participation

The Contractor shall generate reports and attend and participate in meetings including: a Post Award Conference (PAC), (IPTs, Government In-Process Reviews (IPRs), and other program and technical meetings as necessary. The Contractor shall also lead the meetings and working groups when required. The Contractor shall deliver meeting agendas and documentation as specified in: **CDRL B004,** Conference Agenda**,** and **CDRL B005,** Report, Record of Meeting Minutes**.**

4.5.1 Post Award Conference Attendance

The Contractor shall attend and participate in a Government-scheduled PAC following award of this contract task in which the Contractor's lead management, functional, technical, and contractual personnel shall be in attendance, and the meeting shall be conducted IAW FAR Subpart 42.5. The Government will prepare a draft agenda, and the Contractor shall prepare and deliver the final agenda and document the Meeting with the Minutes and Attendance, IAW **CDRLs B004 and B005**.

4.6 Government Furnished Property/Equipment (GFP/GFE)

The current system consists of Government provided hardware and software that the Contractor shall use for modernization efforts and the TFMMS Web sustainment tasking. Hardware will remain under Government inventory control. Software licenses will be tracked and maintained by the Government. The Government will provide the Contractor access to Navy and associated DoD mandatory courseware, and any supporting documents, publications, and technical manuals required for the performance of the contract task. As required by this effort, one or both of the forms, Attachments (4) and (5) shall also be filled out, as needed (by Government or Contractor), and the required GFP/GFE item identification data elements shall be specified.

The Contractor shall use GFE in the test environment to support test and evaluation activities. The current development, test, and production environments will be located at a Government Application Host Facility.

The Contractor shall acknowledge receipt of all GFP/GFE in the GFP, Status and Management Report, **CDRL B006**, and notify the Government of any concerns and risks they identify related to the receipt of GFP/GFE. The Contractor shall maintain a master record showing the disposition and version of the items held.

4.7 Contract Transition Support

The Contractor shall, in addition to any follow-on responsibilities with respect to TFMMS tasks, provide all the software, data, and documentation needed to support a smooth transition to the successor Contractor for follow-on contract support by providing reasonable levels of data and support sufficient to the successor's understanding of the underlying system structure, source code, architecture, and business rules. As part of the transition support, the Contractor shall deliver the latest version of the source code to the Government. This transition support shall be briefly summarized as part of the Contractor's Progress, Status, and Management Report, **CDRL B001**, and software delivered in accordance with Computer Software Product End Items, **CDRL A00C**.

4.8 Limitations on Subcontracting

The FAR Limitation of Subcontracting clause, 52.219-14, requires the Prime to provide at least 50% of the labor costs. The method SPAWAR shall use to track compliance is to require the contractor, through submission of **CDRL B008**, to report, every three months, the % of subcontracted labor costs. This can be tracked by the Government and corrections made to ensure the contract ends up with the Prime performing 50% of the labor costs in-house.

Instructions for completing the CDRL: 1) Identify whether the subcontracting methodology is a percent of contract value or percent of subcontracted value; 2) Identify the subcontracting credit (Tier 1, Tier 2, Tier 3, or All Tiers) in accordance with task order; 3) Identify all subcontractors by name, socio-economic categories, prime vendor purchase order number, percentage of contract value or percent of subcontracted value whichever is applicable, dollar amount, NAICS code to include a description of significant events and how they were a benefit to small business (IAW CPARS Guidance - Attachment A2-2); and, 4) Identify the total percent of contract value or percent of subcontracted value, whichever is applicable, that was expended. The Government reserves the right to perform spot checks and/or request copies of supporting documentation.

BLOCK 12 & 13: The Contractor shall deliver the initial monthly report 105 DACA. Subsequent submissions due no later than 15 days after the end of the next three month period. The required reporting covers every three month period and is an accumulation of the subcontracting efforts to date. The subcontracting information in this report shall be provided in accordance with 52.219-14 as prescribed in 19.508(e) or 19.811-3(e).

4.9 Contractor Work Breakdown Structure (CWBS)

In development of the CWBS, the Contractor shall identify Contractor activities at lower levels (e.g., labor categories, hours, quantities, function points, etc) of resources associated with to the lowest CWBS levels. The Contractor shall maintain the CWBS and additionally shall identify changes to it in the monthly Progress, Status, and Management Report. The below is required Level 1 CWBS.

- Requirements Analysis
- Design

- Development
- Integration
- Testing
- Deployment

5 Technical Requirements

The following requirements are applicable to each delivery of TFMMS Web including: Phase I, Phase II, and sustainment/maintenance updates.

5.1 Software Engineering Development Methodology and Approach

The Contractor shall define a software development approach appropriate for the development and modernization efforts to be performed under this PWS. This overall approach shall be documented in an SDP that shall be IAW the TEP Guidebook. The Contractor shall submit the SDP IAW **CDRL A001** and follow it for all software components to be developed/modified under this effort.

The SDP shall define the Contractor's proposed life cycle model and the processes used as a part of that model. In this context, the term "life cycle model" is as defined in IEEE/EIA Std. 12207.0. The SDP shall describe the overall life cycle and shall include primary, supporting, and organizational processes based on the work content of this solicitation and as placed on the task. In accordance with the framework defined in IEEE/EIA Std. 12207.0, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. Because IEEE/EIA Std. 12207 does not prescribe how to accomplish the task, the Contractor must provide this detailed information so the Government can assess whether the approach is viable.

The SDP shall contain the information defined by IEEE/EIA Std. 12207.1, section 5.3.1 (generic content) and the Plans or Procedures in Table 1 of IEEE/EIA Std. 12207.1. In all cases, the level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted. Information provided must include, as a minimum, specific standards, methods, tools, action, strategies, and responsibilities associated with development and qualification.

5.1.1 Department of Defense (DoD) Guidance

Software development shall support the DoD Net-Centric Data Strategy and Information Enterprise Architecture. Software designs and development shall consider integration or conformance with other Navy and PMW 240 enterprise applications.

5.1.2 Foundational Capabilities

The Contractor shall develop technology and data recommendations to support Government transformation roadmaps, which will be defined by the Government, taking into account factors that include the following:

- Ease of implementation (speed to deploy)
- Total Ownership Cost (TOC)
- Impact to other systems and organizations

- Initiative dependence/independence
- Risks
- Balance between short-term and long-term goals
- Return on Investment (ROI)
- Maintainability and scalability
- Convergence and consolidation opportunities (system rationalization)
- Increased automation

5.2 Systems Engineering

The Contractor shall perform the necessary tasks to evolve the requirements into a finished product. The Contractor shall follow the System Engineering Plan (SEP), provided as Government Furnished Property that describes the Contractor’s overall use of systems engineering throughout the project’s life-cycle, as well as the tools and processes to be used for managing system development. The Contractor can provide suggested revisions to the SEP to the Government for approval and update.

5.3 Technical Reviews

The Contractor shall conduct Technical reviews IAW the TEP guide for each Phase and Post Production Release at the direction and timing of the Government. The Contractor shall support the technical reviews and deliver the documentation identified in Table 1 IAW associated CDRLs. In addition to the CDRLs, the Contractor shall support presentation of additional information, such as the RTM (reported using PMW240 requirements management tool), IAW the TEP guide for each event. These events and deliverables are applicable to each phase of development; although updates to documentation from Phase I is acceptable rather than all new documentation for Phase II.

The Contractor shall provide and conduct the following product, process, and status reviews as defined in the IMS: SRR, SFR, PDR, Critical Design Review (CDR), ATRR, Test Readiness Review (TRR), and Production Readiness Review (PRR). Additionally, the Contractor provides input for the update of the Systems Engineering Management Plan (SEMP) as well as all SE documents and test cases needed for testing and technical reviews, and all DOD Architecture Framework (DoDAF) views.

At a minimum, the OV-1, SV-1, SV-6, DIV-1, DIV-2 and DIV-3 DODAF 2.0 views shall be developed and updated for design and development activities. Other DODAF views may be necessary to support the development of other technical documentation. DODAF Views shall be delivered IAW **CDRL A005.**

Technical Review	CDRL Descriptions	CDRL
System Requirements Review (SRR)/ System Functional Review (SFR)	Software Development Plan (SDP) [final] System/Subsystem Specification (SSS) [final] System Requirements Specification (SRS) [draft]	A001 A002 A003

Preliminary Design Review (PDR)	SRS [final]	A003
	Software Transition Plan (STrP) [draft]	A006
	Software Design Description (SDD)	A004
	DODAF System Architecture Views (OV-1, SV-1, SV-6, DIV-1, DIV-2, DIV-3) [draft]	A005
Critical Design Review (CDR)	SDD [final]	A004
	Interface Control Document (ICD) [draft]	A00A
	STrP [update]	A006
	SSS [update]	A002
	DODAF Views [Final]	A005
	Revisions to SDD, SRS, SDP if required	A001,3,4
Application Unit Testing (AUT) prep	SDP [update] – including: AUT Plan (completed) Quality Assurance (QA) Checklist (completed) AUT Test Cases (completed) Software Product End Items Software Version Description (SVD)	A001 A00C A00D
Application Test Readiness Review (ATRR)	STrP [final]	A006
	Software Operational Verification Test (SOVT) Plan	A007
	Systems Guides/Technical Manuals [draft]	D003, E001
	Software Product End Items [update]	A00C
	SVD	A00D
Production Readiness Review (PRR)	ICD [final]	A00A
	Systems Guides/Technical Manuals [final]	D003, E001
	Software Product End Items [final]	A00C
	SVD [final]	A00D

Table 1 - Technical Events and Associated Deliverables

5.4 IT System Delivery

The Contractor shall deliver successfully tested and finalized executable software and source code IAW the Software Product End Items **CDRL A00C**. The Contractor shall deliver a SVD IAW **CDRL A00D** for each software release.

5.4.1 Manuals and Supplemental Data Delivery

The Contractor shall deliver updated software manuals and documentation including COTS software used in the development of TFMMS Modernization IAW **CDRL E001,** Evaluation of COTS manuals and preparation of supplemental data.

5.4.2 Software Instances

The Government intends to install unique instances of all required software to operate on separate development, test, and production servers in a primary environment located at SSC LANT NOLA and also on separate development, test, and production servers in a failover environment at SSC PAC San Diego. In the failover environment, the Government operating concept is to have the software installed, but inaccessible to users until a failover event occurs. At that time, the failover site becomes active and accessible to users and the primary site is shut down. Data is replicated no less frequently than daily from the primary to the failover site and if the software has to be active for this to occur, the offeror must annotate this in their licensing agreements or exclusions. All licensing agreements and/or exclusions, regardless of the pricing method chosen (e.g. named user, concurrent users, CPU, server, rack, core) must allow for this operating construct with regard to the Government's right to install and use the software.

5.5 Configuration Management (CM) Program

The Contractor shall implement a CM Program as described in the Contractor’s Configuration Management Implementation Plan for the program. The CM Program shall include Baseline Management, Configuration Identification, Configuration Item/Computer Software Configuration Item Identification, CRs, CM Records/Reports, and Configuration Verification and Auditing. All items shall be delivered IAW the applicable CDRLs.

5.6 Logistics Support

5.6.1 Integrated Logistics Support (ILS) Program

The Contractor shall establish an ILS program as specified by DODI 5000.2 and SECNAVINST 5000.2 to ensure that supportability design criteria and characteristics are considered and incorporated into the system design and that the system will meet the operational availability, maintainability, training, and manning requirements established the program’s Functional Requirements Document (FRD). The Contractor shall designate an ILS Manager, establish and update a detailed ILS project schedule as part of the IMS, and participate in Logistics IPT meetings with Government representatives. The Contractor’s ILS activities shall further develop and deliver the ILS related products and data detailed in the paragraphs below as appropriate for individual task orders. The Contractor shall develop a Life Cycle Sustainment Plan (LCSP) that addresses the product support elements supportability strategy in accordance with **CDRL D001**. The Contractor shall develop a Reliability, Availability, and Maintainability Program Plan that addresses how the software baseline requirements will be achieved. The Reliability, Availability, and Maintainability Program Plan shall be delivered in accordance with **CDRL D002**.

5.6.2 System Documentation

The Contractor shall develop and continuously update the Systems Start-up, Systems User, and Systems Administrator Manuals to reflect underlying software coding and architecture, as well as any changes resulting to that baseline throughout the system's lifecycle. For each configuration, the Contractor shall develop and document software user information and the appropriate consolidated operations information that fully supports software load procedures, system initialization, and non-tactical operations. The Contractor shall include information for all system and equipment-oriented instructions necessary to support the Operations & Maintenance (O&M) aspects of the software products in the baselines, to include at a minimum:

1. System software load procedures
2. System initialization procedures

The Contractor shall apply the QA process identified in their Management Plan to each document before it is submitted to the Government. The Contractor shall prepare the System Start-Up Document and System Administration Guide (SAG) in accordance with **CDRL D003**.

5.6.2.1 Validation Report

The Contractor shall deliver a Validation Report in concert with delivery of the System Start-Up Document and/or System Administration Guide (SAG). The Validation will verify procedures in program documentation are accurate and match the operation / maintenance of the system. The validation of system documentation will be conducted during a System Operation Verification Test (SOVT). The Contractor shall support the execution of a SOVT during major software delivery (Test Readiness Review, Production Readiness Review, Quarterly Software Release, etc). The Validation Report will be delivered IAW **CDRL D004.**

5.6.2.2 Commercial-Off-The-Shelf (COTS) Manuals and Supplemental Data Delivery

The Contractor shall assess the adequacy of all COTS manuals supplied along with any supplemental information required to operate and maintain the system. The Contractor shall deliver manuals and documentation for any software or system used in developing the system, and any COTS manual inadequacy reports associated with the system in accordance with **CDRL E001.**

5.6.3 Software Problem Reports (SPR)

During testing or general operation of TFMMS Modernization, anomalies or other unexpected system behavior against fielded software baselines will be documented and routed in SPRs to the Contractor. The Contractor shall provide technical analysis of SPRs filed against fielded software baselines IAW guidance and direction as specified in this task. The Contractor shall provide support to include:

- Addressing configuration issues in coordination with the installation teams and support agencies as needed;
- Working baseline software issues via change request processes based on feedback from software developers;
- Following processes stored in the process repository to include change request routing and Software Problem Report/vulnerability checklists;
- Reviewing the technical documentation related to baseline software for accuracy and thoroughness; provide updates as needed;
- Monitoring and receiving notifications when a new vulnerability, order release, or other hardware change has occurred.
- Assisting the Subject Matter Experts to determine which product baselines are affected;
- Submitting a formal CR for each vulnerability affecting software baselines;
- Following the PMW 240 CM Plan for processing theCRs;
- Drafting mitigation Fleet Advisory Messages and Mandatory Security Updates; and
- Posting patches according to Configuration Management process for subsequent Government approval and release.

5.7 Sustainment

5.7.1 System/Application/Database Sustainment

The Contractor shall implement, test, and deliver system maintenance and provide operational support for the TFMMS Modernization applications and databases, and associated interfaces and data exchanges. This includes the processes, procedures, people, materiel, and information required to support, maintain, and operate the TFMMS software applications and associated databases within the existing operating environment. Software/System releases resulting from sustainment activities shall be documented and updated in the appropriate System Documentation.

The Contractor shall ensure that personnel have the experience and training necessary to perform the duties related to the general management and operations of Information Technology (IT). For those personnel that require root level access to network and server infrastructure, the contractor shall provide personnel that are cyber security workforce compliant in accordance with DoD 8570.01-M and certified IAW DFARS Clause 252.239-7001 Information Assurance Contractor Training and Certification.

The Contractor shall perform the services as described in Section 3 of this PWS that include the following types of sustainment and maintenance services:

- Maintenance of existing applications, infrastructure program or initiative
- Corrective software maintenance, including all efforts to diagnose and correct actual errors (e.g., processing or performance errors)
- Corrective interface maintenance and modifications
- Monitoring system performance, identification of broken or obsolete IT equipment needed to continue operations at the current service level

- Tier II Help Desk support services
- Technical support to the hosting facility as needed for database backups to include restoration and at least quarterly validation of these capabilities.
- Notification and renewal of license and support agreements for existing software supporting the application
- Production support to perform daily, weekly, and monthly monitoring of the program production schedules, interfaces, outputs, and operations. This may include correcting customer data input errors, transfers of data, updating reports and distribution requirements, re-running lost reports, and providing authorized system access.
- C&A support; system vulnerability and secure configuration assessment; research of IA requirements, performing IAVA updates, and providing technical guidance to the programs.

Within the Sustainment Services, the Contractor shall also perform design, modification, test, and implementation activities that include:

- Requirements analysis
- Modifications to system functionality
- New and modified metrics and reports
- New and modified interfaces to external systems based on external system changes or changes that are incidental to maintaining operations of the system.
- New and modified auditing and change control tracking features
- New and modified security and privileges models
- New and modified net-centric, web-services based capabilities
- Changes required to reflect new releases of the DoD and DON Enterprise Architectures
- Changes required to support the certification and annual review of defense business systems
- New and modified capabilities to improve data quality and traceability

In addition, the Contractor shall:

- Provide database administration for all GFE in support of the TFMMS Modernization
- Support user acceptance testing of incremental software builds and final capabilities
- Provide training support for product releases as required. The contractor shall also perform an analysis of the number of users impacted, scope, and complexity of each release to determine user impact and make recommendations for training delivery methods.
- Support the configuration control processes associated with prioritizing and adjudicating customer provided requirements.
- Draft, update, and maintain all process and standards documentation for the TFMMS Modernization.
- Update and maintain all systems and Information Assurance (IA) documentation required for an IA Certification and Accreditation (C&A) and for a valid authority

to operate the TFMMS Modernization systems and all associated hardware and software on the network. This includes but is not limited to all testing and all certification and accreditation documentation as required by and IAW the DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)" and the Department of the Navy DIACAP Handbook"

The Contractor shall ensure that each maintenance update/release is fully operational, including proper data exchange for all interfaces. The Contractor shall deliver, for each release, a software package that includes the upgraded software, updated documentation, and instructions for implementation that would allow for the Government or other third party vendor the ability to implement and make the upgraded software fully operational. The Contractor shall deliver all Computer Software Product End Items in accordance with **CDRL A00C**, including source code and a Software Version Description (SVD) as appropriate in accordance with **CDRL A00D.**

5.7.1.1 Change Requests (CR)

The Contractor shall analyze new requests that are identified by the customer or resulting from new or updated DoD or DON policies and instructions. Based on the Contractor's analysis and presentation of the analysis to the Program Office, if a new request is deemed a potential change/enhancement to the existing product, the Contractor shall enter the CR into an automated configuration management tool as mutually agreed to by the Government and contractor. CRs will form the basis of a requirement for change therefore CRs will be tracked as configuration items.

5.7.1.2 Problem Reports/Defects (PR)

The Contractor shall analyze issues/problems that are submitted from multiple resources. Based on the Contractor's analysis and presentation of the analysis to the Program Office, if a new issue is deemed a potential change/enhancement to the existing product, the Contractor shall enter this new issue as a PR into the an automated configuration management tool as mutually agreed to by the Government and Contractor. When a PR is under consideration for a software change it will be elevated to a CR and tracked under that CI. A PR may also be closed by an update to the knowledge base for Tier 1 support or a policy change which further clarifies and resolves the issue to the user COI.

5.7.2 System Support

The Contractor shall perform all the operations and system support activities addressed in Section 3 of this PWS. Additional information for daily operations and Tier II help desk support, the COTS software support, and the support for system backup and recovery is described in the paragraphs below.

5.7.2.1 Maintain the Commercial-Off-the-Shelf (COTS) Software

Contractor shall maintain all COTS software supporting the functionality and maintainability in the software engineering, testing, production, and training environments. This includes installation security patches in support of IAVM, compliance with Navy Computer Tasking Orders (CTOs), STIGs, STIG updates, and only utilizing software that has vendor support.

The Contractor shall monitor the implementation of COTS software to ensure the terms of the license agreements are satisfied. The Contractor shall notify the Government when changes to licenses are needed or at least 90 days in advance of when licenses need to be renewed.

In the case of end of life (EOL) supportability issues for any COTS, the Contractor shall identify new COTS to replace EOL COTS and develop and implement any design changes to integrate the new software while still maintaining the full functionality of the system.

5.7.2.2 Alternate Site and Data/Disaster Recovery Support

The Contractor shall provide support for image builds and data replication as directed by the Government. The Contractor shall support recovery for systems and databases in accordance with the COOP required for the system's Mission Assurance Category (MAC).

It is projected there shall be one planned disaster recovery event per year in addition to unplanned events. The Contractor shall support disaster recovery activities by providing technical assistance with the transition of system data between the primary and secondary sites, validation that system components are operational, and identification and resolution of any software operational issues while at the secondary site.

5.7.2.3 Conduct Daily Operations and Maintenance

The Contractor shall perform daily operations and maintenance as described in Section 3 of this PWS. This includes daily monitoring of production schedules, interfaces, outputs and other operational activities to verify their correct operation. The Contractor shall take action to correct any operational or interface issues promptly coordinating with interfacing partners as appropriate.

5.7.2.4 User Support and Tier II Help Desk Services

The Contractor shall provide User Support ranging from technical participation in resolving trouble tickets to onsite functional support for user training. Participation for these events can be through phone, audio teleconference, interactive web conferencing, video teleconference, email, or on location at the various customer sites. User Support begins at the Tier I supported by Navy 311 and may proceed into Tier II/III, the technical areas, as issues are identified.

The Contractor shall provide Tier II Help Desk support to correct data, provide training (as required), and to record and resolve software defects. This activity may require research of corporate interfaces and working with personnel supporting corporate systems. The Contractor shall provide Help Desk support a minimum of 5 days per week, 8 hours per day. The Contractor shall work with Government or Tier I and Tier III (e.g. COTS vendor support) Help Desk services to resolve problems.

Tier II support is defined as an issue that is reported by the Tier I Help desk but cannot be resolved within the existing knowledge base. This ticket would be referred to the contract technical support staff for remediation and resolution and could result in a Problem Report (PR), Change Request (CR), or an update to the knowledge base.

Tier III support is defined as an issue that requires the contract support staff to request assistance from an external agency such as an interface partner, service partner, or software or hardware manufacturer.

Tier II and Tier III issues shall be reported immediately by e-mail not to exceed 24 hours from initial identification and monthly thereafter until resolution as part of the Contractor's Progress, Status, and Management Report - Monthly Status Report, **CDRL B001**.

5.8 System Upgrades/Modifications

When approved by the Government, the Contractor shall perform software systems engineering that is considered a minor upgrade or modification to the systems. These upgrades or modifications are considered beyond the maintenance break/fix changes associated with regular sustainment and maintenance activities. These types of software systems engineering activities are minor upgrades or modifications in response to Problem Reports (PRs) and Change Requests (CR).

The Contractor shall produce these software modifications IAW PMW 240 Systems Engineering practices, the PMW 240 Technical Event Process (TEP) Guidebook tailored for the specific effort. This can include requirements and design reviews and other activities outlined in Section 3 of this document. This also includes the update of the systems as required for each technical event. The Contractor shall apply the proper quality control and configuration management needed to perform these upgrades/modifications. All systems documentation shall be developed or updated IAW the associated CDRLs.

The Contractor shall ensure that each software modification/release is fully operational, including proper data exchange for all interfaces. The Contractor shall support test and acceptance activities needed for the release of the software. The Contractor shall perform regression testing, performance testing and installation verification. The Contractor shall provide automated regression testing scripts, IAW **CDRL A00G**, and perform regression testing to ensure that new software releases do not beak existing system functionality. Testing should represent a complete systems test performed by a Quality Assurance (QA) or Test team.

The Contractor shall coordinate with PMW240 training representatives to support the update of all the necessary documentation to support training appropriate for the software change.

The Contractor shall deliver, for each release, a software package that includes: the upgraded software; updated systems, logistics and training documentation (as required); and instructions for implementation that would allow for the Government or other third party vendor the ability to implement and make the upgraded software fully operational. The Contractor shall delivery all Computer Software Product End Items IAW **CDRL A00C**, including a Software Version Description (SVD) as appropriate IAW **CDRL A00D**.

5.9 System Performance

The Contractor shall design TFMMS Modernization to optimize total system performance and minimize degradation. The Contractor shall recommend software performance specifications and minimum host system and network requirements for inclusion in Service Level Agreements (SLAs) to provide an improved, more automated user experience. The Contractor shall design and develop TFMMS Modernization IAW the Key Performance Parameters (KPP) that will be finalized upon completion and approval of the SSS.

As part of sustainment activities, the Contractor shall coordinate with the representatives of the hosting facility as needed and ensure that system performance is maintained as identified by the KPPs. The Contractor shall report on performance metrics as part of the Contractor's Progress, Status and Management Report (**CDRL B001**).

5.9.1 Key Performance Parameters (KPP)

Table 2 reflects the draft TFMMS Web KPPs including threshold and objectives. KPPs will be finalized upon approval of the SSS. The Contractor shall notify the Government of any KPP or Key System Attribute (KSA) that failed (or is failing) to achieve the allocated threshold. KPP "failures" shall be reported within 24 hours and KSA's within five (5) days. Both shall be followed up in writing in the form of a KPP/KSA Failure Reporting.

Requirement	Threshold	Objective
Communication Infrastructure	100% Compliance (Availability to NMCI, RSN, OCONUS)	100% Compliance (availability to NMCI, RSN, OCONUS)
Security	100% Compliance with all security requirements.	100% Compliance with all security requirements.
Concurrent Users	System shall allow for a minimum of 300 concurrent Users without degradation of system performance.	System shall allow for a minimum of 500 concurrent Users without degradation of system performance.
Transaction Accuracy	98% Success	100% Success
System Reliability	Edit failures versus User's input errors in transmitted data that are not detected automatically and require field level manual intervention to correct: +/- 2% of all transactions.	Edit failures versus User's input errors in transmitted data that are not detected automatically and require field level manual intervention to correct: +/- 2% of all transactions.
System Availability	Available 24x7 (95% success)	Available 24x7 (98% success)
Mean Corrective Maintenance Time for Operational Mission Failures (MCMTOMF)	24hr	12hr
Reporting	System must generate, populate, and display simple reports within 10 seconds and complex reports within 2 minutes.	System must generate, populate, and display simple reports within 5 seconds and complex reports within 15 seconds.
Queries	System must have the ability to execute simple queries within 10 seconds and complex queries within 15 seconds.	System must have the ability to execute simple queries within 5 seconds and complex queries within 10 seconds.

Requirement	Threshold	Objective
Screen Refresh	System shall have the ability to perform a screen refresh invoked by the User within 15 seconds of submission.	System shall have the ability to perform a screen refresh invoked by the User within 3-10 seconds of submission.
Navigation	System shall have the ability to navigate between hierarchy levels while utilizing the map within 10 seconds of each instance of level change.	System shall have the ability to navigate between hierarchy levels while utilizing the map within 2 seconds of each instance of level change.

Table 2 – TFMMS Web Key Performance Parameters

5.9.2 Reliability and Maintainability

Reliability and Maintainability are engineering design characteristics for increasing effectiveness and increase performance measures such as operational availability/readiness, dependability (probability of mission success), and safety for users; while decreasing the demand for (and cost of) logistics support.

5.9.3 Data Access and Retrieval

The Contractor shall design TFMMS Modernization such that users are able transfer data within standard Threshold and Objective parameters as defined by the functional requirement. This access and retrieval capability shall be designed in a manner that reflects a representative daily peak operational load with the application scaled and accounting for external network performance and client configuration.

5.10 System Audit Trail

The Contractor shall design TFMMS Modernization with a capability to recall and trace transactions, inputs, processes, or changes, from source to final disposition as required by law or policy.

5.11 Software and Data Transition

The Contractor shall develop a detailed STrP IAW **CDRL A006,** defining the method by which software and operations will be transferred from existing systems into TFMMS Modernization. The Contractor shall include a plan for System Data Migration within the STrP which will support the modernization. The Contractor shall execute these plans to migrate data from existing systems to TFMMS Web prior to legacy system decommissioning. The plan shall minimize the amount of downtime, and be outside of peak manpower periods.

5.12 Interface Development and Maintenance

The Contractor shall configure TFMMS Web such that the system will support external interfaces as identified in the FRD.

The Contractor shall update existing interfaces and required new interfaces with the capability of error handling.

5.12.1 Interface Documentation

The Contractor shall develop or update ICDs IAW **CDRL A00A** for each TFMMS Modernization interface. IRS shall be included in the SRS. Interface Design Documentation shall be included is the SDD.

5.13 Human Systems Interface (HSI) Plan Development

The Contractor shall prepare a HSI plan, **CDRL A00F**, describing the processes and procedures for ensuring the TFMMS Modernization adheres to HSI best practices. The HSI Plan shall be delivered in accordance with CDRL. The Contractor shall also interface with Government-designated HSI subject matter experts (SMEs) prior to PDR and incorporate any Government-directed value-added changes that enhance the system within existing scope, budgetary, and schedule constraints of the contract.

5.14 Technology Insertion

The Contractor shall assess and make recommendations for implanting new technology to improve product capabilities, mitigate program risk, and reduce total ownership costs.

6 System Security

6.1 General Information Security Requirements

The Contractor shall deliver and/or maintain an accredited system in accordance with DoDI 8510.01 - Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) and/or and the following guidance:

- Subchapter III of Chapter 35 of title 44, United States Code, “Federal Information Security Management Act (FISMA) of 2002”
- DoD Directive 8500.01E, “Information Assurance (IA),” October 24, 2002
- DoD Directive 8100.1, “Global Information Grid (GIG) Overarching Policy,” September 19, 2002
- DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
- Director of Central Intelligence Directive 6/3 (DCID 6/3), “Protecting Sensitive Compartmented Information Within Information Systems,” May 24, 2000
- DON Information Security Program SECNAV M-5510.36, June 2006

The Contractor shall implement all Information Assurance (IA) controls, not specified by the Government as inherited, and as defined within DoD Instruction 8500.2 in accordance with the MAC and confidentiality level of information processed, stored, or communicated.

The Contractor shall establish DoDI 8500.2 compliant administrative/operational, technical, and physical/environmental safeguards to protect any and all Government systems and data to ensure the confidentiality, integrity, availability, authentication, and non-repudiation of Government information. At a minimum, the safeguards shall include provisions for personnel security, electronic security and physical security, including access to Sensitive, Classified, Privacy Act data.

The contractor shall ensure all appropriate security investigations required by DoD regulations and Secretary of the Navy directives and instructions are accomplished for personnel assigned to this effort. The Contractor shall ensure that TFMMS Modernization assets have been secured according to all DISA prepared STIGs, Security Requirements Guides, and other DoD mandated secure configuration guides during the development, test, deployment, and maintenance. At a minimum, the Application Security and Development, Operating System, Database, and Web Server STIGs are met. If there is software that is outside of the scope of these STIGs, additional DoD/DON security guidance will be reviewed and implemented to ensure the program is compliant with current DoD/DON guidance.

The Contractor shall ensure that the TFMMS Modernization is able to operate within a Government approved location which has been configured to meet all applicable STIGS and IAVA. The Contractor shall ensure that TFMMS Modernization shall integrate third party anti-virus and Host Based Security software as required by DoD and DON.

The Contractor shall demonstrate compliance with policy guidance for International Common Criteria (ICC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the Navy Information/Application Product (NIAP) Evaluation and Validation Program, the Federal Information Processing Standards (FIPS) validation program, use of Mobile Code Technologies in DoD Information Systems and the Navy Ports, Protocols, and Services (NPPS) Manual.

The Contractor shall provide technical and project management support related to all aspects of the Clinger-Cohen Act of 1996, and specifically the requirements of IA. This includes participation in technical reviews and analyses of capability, processes and systems. Results of analyses and recommendations shall be provided to the PCO or Contracting Officer Representative (COR) within 20 calendar days of completing the analyses.

6.2 Certification & Accreditation (C&A)

C&A requirements apply to all DoD and Contractor's Information System (IS)/networks that receive, process, display, store, or transmit DoD information. The Contractor shall comply with the C&A process for implementing information safeguards. The C&A process will be used to obtain Authorities to Operate, Interim Authorities to Operate and Authorities to Test to support the program requirements.

The C&A requirements shall be met prior to allowing TFMMS Modernization authorized access to DoD data or interconnect with any DoD IS/network that receives, processes, stores, displays or transmits DoD data. The Contractor shall support the C&A process by providing the PCO the required documentation necessary to receive an Approval to Operate (ATO). The Contractor shall make IS/networks available for testing, and support the C&A testing in advance of accessing DoD data or interconnecting with DoD IS/networks. The Contractor shall ensure Contractor support staff is available to participate in all phases of the C&A process, including, at a minimum:

- Attending and supporting C&A meetings with the Government
- Supporting C&A package development/submission.
- Supporting/conducting the vulnerability mitigation process

- Supporting the C&A Team during system security testing
- Supporting maintaining, monitoring and validating of security posture

Contractors must confirm that IS/networks are secured and baselined prior to initiating testing. Confirmation of system baseline shall be agreed upon during the definition of the C&A boundary and be signed and documented as part of the C&A Plan. Baselining the system means that there shall be no changes made to the configuration of the system (within the C&A boundary) during the C&A process.

Any re-configuration or change in the system during the C&A testing process will require a re-baselining of the system and documentation of system changes.

Vulnerabilities identified by the Government as "must-fix" issues during the C&A process must be mitigated according to the timeline identified by the Information Assurance Manager (IAM), Information Assurance Officer (IAO), or Designated Approving Authority (DAA). DoD developed checklists, reference materials, and C&A tools may be obtained from the DISA IASE website at http://iase.disa.mil/index2.html. Utilities, reference material and configuration guides are provided at this site.

The Contractor shall submit C&A documentation IAW existing procedures and regulations and as specified in **CDRL A00E**.

6.3 Information Assurance Vulnerability Management (IAVM)

The Contractor shall implement an IAVM program to comply with the Navy IAVM process and report both IAVM and Communication Tasking Order (CTO) compliance to the Navy’s Tier 2 Computer Network Defense Service Provider (CNDSP), Navy Cyber Defense Operations Command (NCDOC) to provide CND and Network Operations (NetOps) visibility to Navy leadership.

The Contractor shall inspect TFMMS Web assets for vulnerabilities through manual checklist reviews and automated scanning tools using Government approved products. Currently, the scanning product is eEye Retina.

The Contractor shall apply vendor software patches in accordance with IA Control VIVM-1 on at least a monthly basis and with serious vulnerability issues dealt with ASAP.

6.4 Data Protection

The Contractor shall comply with the DON Privacy program per SECNAVINST 5211.5E.

The Contractor shall ensure all categories of sensitive information, including Personally Identifiable Information (PII), are secured and in compliance with all IA Controls from the DoDI 8500.2, specifically IA Controls DCFA-1 and DCSR-2. Compliance includes the encryption of “data in transit” and “data at rest” as required by the data owner.

The Contractor shall comply with DON CIO MSG DTG 171952Z APR 07 to ensure that all PII is properly safeguarded. The requirement under the E-Government Act of 2002, mandates that all PII be protected. In addition, systems processing PII must have completed a Privacy Impact Assessment (PIA) and register that PIA with DON CIO.

The Contractor shall provide controlled access to prevent unauthorized access to DoD systems and information using identification and authentication as well as encryption.

6.5 Personnel Security

In addition to the personnel requirements outlined in the DoDD 8500.01E and DoDI 8500.2, the Contractor shall comply with the DoD 5200.2-R, "Personnel Security Program Requirements."

Contractor personnel performing work under this contract must have a minimum of a Secret clearance prior to commencement of work under this contract, and must maintain the level of security required for the life of the contract. The security requirements are in accordance with the DD 254, Department of Defense Contract Security Classification Specification.

Contractor responsibilities for ensuring personnel security shall include, at a minimum, meeting the following requirements:

- Initiate, maintain, and document personnel background investigations appropriate to the individual's responsibilities and required level of access to systems/information.
- Immediately report and deny access to any IS, network, or information if a Contractor employee filling a sensitive position receives an unfavorable adjudication. Access denial may occur if information that would result in an unfavorable adjudication becomes available, or if directed to do so by the PCO or COR for security reasons.
- Ensure all Contractor personnel receive IA training before being granted access to DoD AISs/networks, and/or information. IA awareness training will be completed annually. Contractor personnel will participate in IA standdowns and any additional mandated periodic IA awareness training.
- Ensure all Contractor personnel demonstrate a “need to know” prior to being granted access to DoD AISs/networks, and/or information.

Contract personnel supporting TFMMS Modernization who are performing IA functions that are designated as IA Workforce positions IAW DoD 8570.01-M shall be trained and certified in accordance with DFARS Clause 252.239-7001 Information Assurance Contractor Training and Certification. The Contractor shall follow SECNAVINST 5239.3A of 20 Dec 2004 & DoD 8500.2 of 6 Feb 2003 when performing IATOs.

6.6 Incident Response

Timely detection and rapid response to suspected or confirmed security incidents are essential in order to identify and contain any breach to IA. The Contractor shall demonstrate to the customer sufficient policies, processes, and resources available to support an Incident Response Program (IRP). The IRP shall support capabilities comparable to those identified in relevant DoD and DON policy or other accepted and documented commercial "best practices" (e.g., National Institute of Standards and Technology (NIST) standards or similar).

In the event of an incident the Contractor shall:

- Notify the Government within 24 hours in the event of a confirmed security incident, or within 48 hours of a suspected security incident, that impacts or potentially impacts customer systems, networks, or data.
- Shall agree with the Government to share information regarding any security incident sufficient to:
    - identify the cause of the security incident (i.e., attack vector and methodology)
    - identify the technical or procedural vulnerabilities that allowed the incident to occur
    - identify any unauthorized actions taken with respect to the relevant systems, networks, or data in question
- Shall mutually agree with the Government upon actions and other measures to be taken to mitigate vulnerabilities associated with the incident and to ensure that similar incidents do not recur.

6.7 Wireless Technologies

While improving productivity and providing greater flexibility for employees, wireless technologies, if not properly secured, can also introduce significant security vulnerabilities that may jeopardize the confidentiality, integrity, and/or availability of systems, networks, and data. Wireless technologies include at a minimum, Wireless Local Area Networks (WLANs), Wireless Personal Area Networks (WPANs), and Wireless Portable Electronic Devices (PEDs).

Government systems, networks, or data shall NOT be connected to or placed on Contractor systems or networks that utilize wireless technologies, unless the following conditions are met:

- The Contractor shall ensure that all wireless technologies are procured, configured, and maintained in accordance with applicable DoD and DON wireless policies and configuration guides or with comparable accepted and documented commercial "best practices." Guidance is not limited to the following:
    - DoD Commercial Mobile Device (CMD) Interim Policy, Jan 17, 2012
    - NIST Wireless Security Guidance SP 800-48, Dec 4, 2002
    - DoDI 8420.01, Nov 3, 2009
    - Pentagon Wireless Security Policy, Sep 25, 2002
    - Wireless STIG, (Current release)
- The Contractor shall demonstrate to the Government that wireless technologies are in compliance with the policies and standards referenced above.

6.8 Disposing of Electronic Media

The Contractor shall comply with DoD standards and procedures and shall use approved products to dispose of unclassified hard drives and other electronic media in accordance with DoD Memorandum "Disposition of Unclassified Computer Hard Drives," June 4, 2001, and to dispose of classified hard drives and other electronic media in accordance with CNSS Instruction 4004.1 "Destruction and Emergency Protection Procedures for COMSEC and Classified Material," April 2007.

The Contractor is further required to follow DOD guidance on sanitization of other internal and external media components in accordance with DODI 8500.2 "Information Assurance (IA) Implementation," 6 Feb 2003 (see PECS-1 in enclosure 4 Attachment 5) and DOD 5220.22-M "Industrial Security Program Operating Manual (NISPOM)," (Chapter 8).

6.9 Ports, Protocols, and Services (PPS)

The Contractor shall comply with all current DoD and DISA standards and requirements for acceptable PPS. Any request for exception to these requirements must be made through the Program Manager to the DAA. Management of PPS is governed by DoDI 8551.1 and the Navy Ports, Protocols, and Services (NPPS) Manual, Version 1.5, November 16, 2010.

6.10 Public Key Infrastructure (PKI) and Encryption

The Contractor shall comply with DoD standards, policies, and procedures related to the use of PKI certificates and biometrics for positive authentication. Where interoperable PKI is required, DoD issued certificates, for the exchange of unclassified information between DoD and the Contractor shall obtained. The Contractor must turn over to the Government all encryption keys for deployed systems, backdoor algorithms, and procedures for use in remote support. The Contractor must provide a written report detailing all encryption related materials prior to contract expiration, regardless of modifications or extensions.

6.11 Information Systems (IS)/Networks Physical Security

The Contractor shall employ physical security safeguards for IS/Networks involved in processing or storage of Government Data. The safeguards, conforming to DoD regulations, shall prevent the unauthorized access, disclosure, modification, or destruction of Government data. In addition, the Contractor will support a Physical Security Audit (PSA) of the Contractor's internal information management infrastructure, performed by the Government. The Contractor shall correct any deficiencies of the Contractor's physical security posture identified by the Government.

6.12 Non-Classified Internet Protocol Router Network (NIPRNet)/Secret Internet Protocol Router Network (SIPRNet) Connection Criteria Policy

The Contractor shall comply with DISN Connection policy (CJCSI 6211.02B) for any connections to NIPRNet and SIPRNet.

6.13 DON Applications & Data Management System (DADMS)

The Contractor shall ensure that all deliverables include Functional Area Management (FAM) approved applications. The Contractor shall ensure that all databases that use Database Management Systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DADMS and are FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on a Research, Development, Test & Evaluation (RDT&E) network.

6.14 DoD Information Technology Portfolio Repository (DITPR)

The Contractor shall ensure that all networks and systems procured and/or connected to a Navy network complete DITPR-DON registration and receive FAM approval.

6.15 Options for the Software Process Improvement Initiative (SPII) language

Individual contract requirements documentation shall invoke the standards of the ASN Software Process Improvement Initiative (SPII) Guidance for Use of Software Process Improvement Contract Language, 13 July 2007" or "Use best industry practices including ISO/IEC 15288 for System life cycle processes and ISO/IEC 12207 for Software life cycle processes. In accordance with the framework defined in IEEE/EIA Std. 12207.0, the Software Development Plan (SDP) shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks. The best practices represented in the CMMI - SE/SW model shall be used for all systems and software engineering projects and tasks. All system-software development will be in accordance within the CMMI Level 3.

6.16 Mission Assurance Category and Sensitivity

The Contractor shall ensure the system is developed to meet the Mission Assurance Category (MAC) II Sensitive and Classified controls as defined in DoDI 8500.2 Enclosure 4 Attachments 2, 4, and 5. IA requirements are applicable for the development of portal guidance for integration of applications and for the development of the TFMMS.

7 Appendix A: Acronyms

AFT	Application Functional Testing
AIS	Automated Information System
AMM	Activity Manpower Management
A_O	Operational Availability
APM	Assistant Program Manager
ASAP	As Soon As Possible
ASCA	Administrative Simplification Compliance Act
ASN	Assistant Secretary of the Navy
ASIT	Application System Integration Testing
ATO	Authority to Operate
ATRR	Application Test Readiness Review
AUT	Application Unit Testing
AV	All Viewpoint
BPR	Business Process Reengineering
C&A	Certification & Accreditation
CCB	Configuration Control Board
CDAD	Contractor Performance Assessment Report Systems (CPARS) Draft Approval Document
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CFSR	Contract Funds Status Report
CI	Configuration Item
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CLIN	Contract Line Item
CM	Configuration Management
CMD	Commercial Mobile Device
CMIP	Configuration Management Implementation Plan
CMMI - SE/SW	Capability Maturity Model Integration for Systems Engineering and

Software Engineering

CMP	Configuration Management Plan
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COA	Course of Action
CONUS	Continental United States (excludes Alaska and Hawaii)
COOP	Continuity of Operations
COR	Contracting Officer Representative
COTS	Commercial-Off-the-Shelf
CPARS	Contract Performance Assessment Reporting System
CR	Change Request
CRD	Capability Requirements Document
CSA	Capabilities Solution Analysis
CSA	Configuration Status Accounting
CSCI	Computer Software Configuration Item
CTO	Computer Tasking Orders
CWBS	Contract Work Breakdown Structure
DAA	Designated Approving Authority
DADMS	DON Applications and Database Management System
DBDD	Database Design Descriptions
DBMS	Database Management Systems
DC	District of Columbia
DCFA	Security Design and Configuration – Functional Architecture for AIS Applications
DCID	Director of Central Intelligence Directive
DCSR	Security Design and Configuration – Specified Robustness
DFARS	Defense Federal Acquisition Regulation Supplement
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIBRS	Defense Incident Based Reporting System
DID	Data Item Description
DISA	Defense Information System Agency
DISN	Defense Information System Network
DITPR-DON	DoD IT Portfolio Repository – Department of the Navy

DIV	Data and Information Viewpoint
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DON	Department of the Navy
DTD	Document Type Definitions
DTM	Directive-Type Memorandum
DUA	Data Use Agreements
EA	Enterprise Architecture
ECP	Engineering Change Proposal
ECR	Engineering Change Requests
EIA	Electronic Industries Alliance
ERD	Entity-Relationship Diagram
FAM	Fleet Advisory Messages
FAM	Functional Area Management
FAM Training	Familiarization Training
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FRD	Functional Requirements Document
GFE	Government Furnished Equipment
GFP	Government Furnished Property
GIG	Global Information Grid
GOTS	Government-Off-The-Shelf
GWBS	Government Work Breakdown Structure
HR	Human Resource
HSI	Human System Interface
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment

IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Alerts
IAVM	Information Assurance Vulnerability Management
IAW	In accordance with
ICC	International Common Criteria
ICD	Interface Control Document
IEEE	Institute of Electrical and Electronics Engineers
IETM	Interactive Electronic Technical Manual
ILS	Integrated Logistics Support
IMP	Integrated Management Plan
IMS	Integrated Master Schedule
INV	Investigations
IPMR	Integrated Program Management Report
IPR	In-Process Review
IPRD	Instructional Performance Requirements Document
IPT	Integrated Product Team
IRP	Incident Response Program
IS	Information System
ISO	International Organization for Standardization
IT	Information Technology
KPP	Key Performance Parameters
KSA	Key System Attributes
LE	Law Enforcement
LMI	Logistics Management Information
MAC	Mission Assurance Category
MSU	Mandatory Security Updates
NCDOC	Navy Cyber Defense Operations Command
NEN	Naval Enterprise Networks
NGEN	Next Generation Enterprise Network
NIAP	Navy Information/ Application Product
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NISPOM	Industrial Security Program Operating Manual
NIST	National Institute of Standards and Technology

NMCI	Navy Marine Corps Intranet
NetOps	Network Operations
NOLA	New Orleans, LA
NPPS	Navy Ports, Protocols, and Services
O&M	Operations & Maintenance
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
OLH	OnLine Help
OPNAV	Office of the Chief of Naval Operations
PAC	Post Award Conference
PCO	Procuring Contracting Officer
PDF	Portable Document Format
PDR	Preliminary Design Review
PECS	Physical and Environmental – Cleaning and Sanitizing
PEO-EIS	Program Executive Office for Enterprise Information Systems
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMW 240	Sea Warrior Program Office
PPS	Ports, Protocols, and Services
PRR	Production Readiness Review
PSA	Physical Security Audit
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QCP	Quality Control Program
RDA	Research, Development & Acquisition
RDT&E	Research, Development, Test & Evaluation
RMP	Risk Management Plan
ROI	Return on Investment
RTM	Requirements Traceability Matrix
SCOM	Software Center Operator Manual
SDD	Software Design Document
SDP	Software Development Plan

SECNAVINST	Secretary of the Navy Instruction
SEP	System Engineering Plan
SFR	System Functional Review
SIPRNEet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SME	Subject Matter Expert
SPAWAR	Space and Naval Warfare Systems Command
SPAWARINST	SPAWAR Instruction
SPII	Software Process Improvement Initiative
SPR	Software Problem Report
SRR	System Requirements Review
SRS	System Requirements Specification
SSAA	System Security Authorization Agreement
SSDD	System/Subsystem Design Document
SSS	System/Subsystem Specification
STIG	Security Technical Implementation Guide
STP	Software Test Plan
STR	Software Test Report
STrP	Software Transition Plan
SV	System Viewpoint
SVcV	Service Viewpoint
SVD	Software Version Description
TEMP	Test and Evaluation Master Plan
TEP	Technical Event Process
TFMMS	Total Force Manpower Management System
TM	Technical Manual
TMMCA	TFMMS Micro Manpower Change Application
TO	Task Order
TOC	Total Ownership Cost
TRR	Test Readiness Review
UAT	User Acceptance Testing
UPK	User Productivity Kit
USMC	United States Marine Corps

USN	United States Navy
VIVM	Vulnerability and Incident Management – Vulnerability Management
WLAN	Wireless Local Area Networks
WPAN	Wireless Personal Area Networks

8 Appendix B: Data Deliverables Matrix

ENGINEERING DATA

Data Item Number	Description	Data Item Description (DID)	PWS Paragraph
A001	Software Development Plan (SDP)– Software Engineering Development Methodology and Approach	DI-IPSC-81427A	3.1.3, 3.1.5, 5.1, 5.3
A002	System/Subsystem Specification (SSS)	DI-IPSC-81431A	2.1, 3.1.1, 5.3
A003	Software Requirements Specification (SRS)	DI-IPSC-81433A	2.1, 3.1.1, 3.1.5,5.3
A004	Software Design Description (SDD)	DI-IPSC-81435A	2.1, 3.1.2, 5.3
A005	DoD Architecture Framework (DoDAF) Documentation	DI-MGMT-81644A	5.3
A006	Software Transition Plan (STrP) – Transition From Existing Systems	DI-IPSC-81429A	5.3, 5.9
A007	Software Test Plan (STP) – System Operational Verification Test (SOVT) Plan	Per SPAWAR Instr & SOVT Guide (GFI)	5.3, 5.6.2.1
A008	Contractor's Configuration Management Implementation Plan – Configuration Management (CM) Plan	DI-CMAN-80858B	4.4
A009	Configuration Status Accounting Information – Configuration Management Records/Reports	DI-CMAN-81253A	4.4.1
A00A	Interface Control Document (ICD) – Interface Control Document (ICD) Development	DI-CMAN-81248A	5.3, 5.10.1, 5.12.1
A00B	Computer Software Configuration Items (CSCIs) List	Per PMW 240 Systems Engineering Process and Example	4.4.2
A00C	Computer Software Product End Items	DI-IPSC-80590B	4.7, 5.3, 5.4, 5.7, 5.8
A00D	Software Version Description (SVD)	DI-IPSC-81442A	4.4.2, 5.3, 5.4, 5.7, 5.8
A00E	Certification & Accreditation (C&A) Documentation	IAW current DoD/DON Guidance	3.1, 6.2
A00F	Human Engineering – Human Systems Integration Plan	MIL-STD-1472G	5.11
A00G	Regression Testing Scripts	With each software version release	3.1.6.2, 5.8

ADMINISTRATIVE DATA

Data Item Number	Description	Data Item Description (DID)	PWS Paragraph
B001	Contractor's Progress, Status, and Management Report - Monthly Status Report	DI-MGMT-80227 & 81468	4.1, 4.1.1, 4.3.2, 4.7, 5.7.2.4, 5.9
B002	Contractor's Progress, Status, and Management Report - CPARS Draft Approval Document (CDAD) Report	DI-MGMT-80227	4.2
B003	Management Plan – Management Plan Development and maintenance	DI-MGMT-80004A	4.3, 4.3.1, 4.3.2, 4.3.3
B004	Conference Agenda – Meeting Agendas Preparation	DI-ADMN-81249A	4.5, 4.5.1
B005	Report, Record of Meeting/Minutes – Meeting Attendance and Documentation	DI-ADMN-81505	4.5, 4.5.1
B006	Government Furnished Property (GFP), Status and Management Report - GFP Monthly Status Report (MSR)	See Block 16 of CDRL	4.6
B007	Integrated Program Management Report (IPMR)/Integrated Master Schedule (IMS)	DI-MGMT-81861	4.1.2
B008	Certification/Data Report -	Subcontracting Status report	4.8
B009	Function Point (FP) Analysis Report	See CDRL Blk 16	4.1.4

LOGISTICS DATA

Data Item Number	Description	Data Item Description (DID)	PWS Paragraph
D001	Integrated Logistics Support (ILS) Plan	DI-ILSS-80095	5.6.1
D002	Reliability Centered Maintenance (RCM) Failure Modes and Effects Analysis (FMEA) Report / Reliability, Availability, Maintainability Program Plan	DI-SESS-81613	5.6.1
D003	Software Center Operator Manual - System Documentation	DI-IPSC-81444	5.3, 5.6.2
D004	Validation Report – SCOM Validation Verification Report	DI-CMAN-80792A	5.6.2.1

PUBLICATIONS MANUALS

Data Item Number	Description	Data Item Description (DID)	PWS Paragraph
E001	Evaluation of Commercial Off-the-Shelf (COTS) Manuals and Preparation of Supplemental Data - Commercial Off-The-Shelf (COTS) Manuals and Supplemental Data Delivery	MIL-PRF-32216 & DI-TMSS-80527B	5.3, 5.6.2.2

9 Appendix C: Applicable Documents

9.1 C1. Government Documents

DoD 5200.2R - Personnel Security Program (Feb 23, 1996)

DoD 5200.2 - DoD Personnel Security Program Requirements (Apr, 09, 1999)

DoD 5220.22-M Industrial Security Program Operating Manual (NISPOM) (Mar 18, 2011)

DoD 5400.11- DoD Privacy Program (May 14, 2007)

DoD 5400.11 - Department of Defense Privacy Program, (Sept 01, 2011)

DoD 6025.18-R- Health Information Privacy (Jan 24, 2003)

DoD 8100.1 -Global Information Grid (GIG) Overarching Policy (Sept 19, 2002)

DoD 8100.4 - Unified Capabilities (UC) (Dec 9, 2010)

DoD 8320.02G - Guidance for Net-Centric Data Sharing (Apr 12, 2006)

DoD 8320.5 Electromagnetic Spectrum Data Sharing (Aug 18, 2011)

DoD 8400.01-M Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations (Jun 03, 2011)

DoD 8500.01E Information Assurance (Oct 24, 2002)

DoD 8500.2 Information Assurance Implementation (Feb 6, 2003)

DoD 8510.10 - Information Assurance Certification and Accreditation Process (DIACAP) (Nov 28, 2007)

DoD 8551.1- Ports Protocols and Services Management (Aug 13, 2004)

DoD 8570.01M - Information Assurance Workforce Improvement Program (Jan 04, 2012)

DTM-07-15 Social Security Number (SSN) Reduction Plan (Dec 15, 2011)

SECNAVINST 5000.36A - Information Technology Applications And Data Management (Jun 14, 2010)

SECNAVINST 5510.30B - Department of the Navy Personnel Security Program (PSP) (Oct 06, 2006)

SECNAV 5211.5E - Department of Navy Privacy Program (Oct 29, 2004)

SECNAV M-5239.2 – Information Assurance Workforce Manual (May 29, 2009)

SECNAV 5239.3 – Information Assurance Policy (Jun 17, 2009)

SECNAVINST 5720.47- Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites (Dec 28, 2010)

ASN RDA Memorandum DON Policy on Digital Product/Technical Data (Oct 23, 2004)

9.2 C2. Government Documents

CJCSI 6211.02B - Defense Information System Network (DISN): Policy Responsibilities and Processes of (Jul 31, 2003)

CJCSI 6212.01F- Net Ready Key Performance Parameter (NR KPP) (Mar 21, 2012)

OPNAV 5239.1C - Information Awareness Program (Aug 20, 2008)

OPNAV Note 5200, Manpower, Personnel, Training and Education Information Services Requirements Integration Implementing Guidance

SPAWAR 4160.3B – Technical Management Data

Copies of the above DoD, SECNAV, and OPNAV instructions are downloadable from) http://doni.daps.dla.mil/allinstructions.aspx).

9.3 C3. Specifications, Standards, & Handbooks

IEEE/EIA 12207-2008 – Standard for Systems and Software Engineering –Software Lifecycle Processes (Jan 31, 2008)

ANSI/EIA 649.B – National Consensus Standard for Configuration Management

ANSI/EIA 836 – Configuration Management – Data Exchange and Interoperability

MIL-PRF-29612B - Training Data Products

MIL-HDBK-29612-2A - Instructional Systems Development/Systems Approach To
Training and Education (Part 2 of 5 Parts)

MIL-HDBK-29612-3A - Development of Interactive Multimedia Instruction (Part 3 of 5)

MIL-HDBK-29612-4 - Glossary (Part 4 of 5)

MIL-HDBK-29612-5 - Advanced Distributed Learning (ADL) Products and Systems (Part5 of 5)

MIL-HDBK-881A - Work Breakdown Structures for Defense Materiel Items

MIL-HDBK-502 - DoD Acquisition Logistics Handbook

MIL-PRF-49506 - Performance Specification Logistics Management Information

(Copies of the above DoD Specification and handbooks can be obtained online from the Acquisition Streamlining and Standardization Information System (ASSIST) Web Site at: http://assist.daps.dla.mil/quicksearch/.)

9.4 C4. Government Regulations

(DONCIO) Section 508 - Self-Help Tool Kit
http://www.doncio.navy.mil/sewction508toolkit

9.5 C5. Other Government Documents, Drawings, and Publications

Possible additional guidance materials include, but are not limited to:

DoD Public Key Infrastructure (PKI) (http://iase.disa.mil/pki/index.html)

DoD Implementation Guide for Transitional PIV II SP 800-73 v1 (Mar 24, 2006) Navy Marine Corps Intranet (NMCI) Release Development and Deployment Guide (NRDDG) v2.0 (May 28, 2004)

Sea Warrior Program Office Technical Event Process (TEP) Guidebook, (Feb 22, 2010)

Sea Warrior Program Office Risk Management Plan, (Feb 12, 2007)

Sea Warrior Program Office Test and Evaluation Master Plan (TEMP), (Mar 24, 2008)

Sea Warrior Program Office Systems Engineering Plan, (Mar 24, 2008)

Sea Warrior Program Office Configuration Management Plan, (Dec 15, 2010)

Sea Warrior Program Office Project Plan User Guide, (Apr 22 2010)

SSC NOLA Service Oriented Architecture (SOA) Technical Reference Model